How Exchange Hides Group Membership on AD

By Marcelo Calbucci

Keywords: Exchange, ADC, Recipient Update Service, Exchange System Management, Non-Canonical Security Descriptor, hideDLMembership, Group Membership, Security.

The Exchange 5.5 has its own Directory Service, so it is responsible to define how people can browse thru attributes and who has the right to read or write certain properties. This make easier for Exchange to decide when somebody could see or not the membership of a group, because the code that show that attribute thru MAPI or LDAP was passing thru Exchange security system.

On Exchange 2000, the Active Directory replaces the Exchange Directory, so all the security system for LDAP queries now belong to Windows 2000, and Windows 2000 give us the power to control access to several levels, including a single attribute.

For that reason, Exchange 2000 uses the Windows 2000 Security Descriptor to control who has and who hasn't the right to see the members of a group.

For instance, all Exchange 2000 installed on your organization need the permission to see the list of members from a Group, even if this Group has the checkbox for Hide Membership checked; otherwise those servers wouldn't be able to "expand" the Group membership and deliver the message.

To give the Exchange user and administrator maximum security possible, the solution to solve this problem depends on 3 components: the Active Directory Connector, the Recipient Update Service and the Exchange System Management snap-in.

Coming from Exchange 5.5

If you are installing Exchange 2000 in a mixed topology, with one or more Exchange 5.5, you will need the ADC to replicates your entries from the Exchange Directory to the Active Directory and vice-versa. For this reason, if you're replicating a Distribution List that has the "hide-dl-membership" attribute set to TRUE, you need to preserve this status on the AD.

To accomplish that, when ADC is replicating this entry, it will detect that it has this attribute set to TRUE, and it will stamp a set of ACEs on the Security Descriptor. Those ACEs will be on a Non-Canonical format, which means that at least one Denied ACE will be after an allowed ACE.

To determine which Security Principals have the right to read/write membership, ADC will read the attribute "msExchServerGlobalGroups" from your Organization Container entry on the AD, and will extract the list of SIDs that will compose the Non-Canonical part of the Security Descriptor.

Here is one example: Your organization has several Exchange 2000 on two different domains, DomA and DomB. You'll have two groups that the Exchange setup creates, called "DomA\Domain EXServers" and "DomB\Domain EXServers". The "msExchServerGlobalGroups" will contain two values, which will be the SID of those two groups.

The final Security Descriptor of that group, after ADC replicates it to AD will be:

Ace #	Type	Right	SID	
1	Allowed	Read/Write Member	DomA\Domain EXServers	Non-Canonical part
2	Allowed	Read/Write Member	DomB\Domain EXServers	Canonical part
3	Denied	Read/Write Member	Everyone	
4	T	A	B	
…				
N-1	X	C	D	
N	Z	E	F	

ADC will add the first to the third ACE. So, when the Windows Security subsystem evaluates this permission it will grant to both Domain EXServers the right to read/write the membership, but nobody else.

When you go to the "Users and Computers" snap-in, and select "Advanced Features" on the "View" menu, you'll be able see the "Security" tab on each entry. If you select the Group that contains the Non-Canonical Security Descriptor, you'll get the following message:

> "Windows can not edit the permissions on 'MyHiddenGroup' because they have been written in a non-standard format by another application. To enable editing, you must use the application to restore the permissions to a standard format."

Basically, the Windows Security subsystem does understand Non-Canonical formats, but the User Interface doesn't let you edit it.

The Recipient Update Service

The solution above has two problems: What if the ADC is running before the first Exchange 2000 server is installed? And What if you add a new domain with Exchange 2000 to your organization, how it would be added to the list of servers on the Non-Canonical Security Descriptor?

The answer for both questions is the Recipient Update Service.

The Recipient Update Service has the job of monitoring changes on the Active Directory and takes actions based on these changes. Mainly, it will add, remove and modify e-mail addresses, address lists, and other attributes for mail-enabled entries, like users, contacts, groups and public folder. But it will also know when a new server and/or a new domain were added to the network.

Specifically if you add a new Exchange 2000 on a domain that didn't had any Exchange 2000 before, it'll search for all groups that have meet the condition "(hideDLMembership=TRUE)" and reset the Security Descriptor to meet the new requirement for the Non-Canonical SD.

As a side effect, if you go manually thru some LDAP interface and change the attribute "hideDLMembership" to TRUE or FALSE, the Recipient Update Service will notice that and add or remove the Non-Canonical part of the Security Descriptor. This let companies to write their own application to change the status of a member-hidden group without compromising security.

Immediate Action

The Recipient Update Service might take a few seconds to identify a new change on the Active Directory, up to a few minutes, depending on several conditions. This few seconds to few minutes can be an eternity for extremely secure aware networks. For that reason, once you selected a group on the "Users and Computers" snap-in, the Exchange Extension for that snap-in will provide immediate action if you choose to hide the membership of that Group.

What you have to do is to select "Exchange Tasks…" and "Hide Membership". This will immediately change the Security Descriptor of that group in order to do not let anybody to access its membership information.

Nobody, means nobody!

Not even the Administrator will be allowed to see or edit the membership of a Group that has hideDLMembership equal to TRUE. In order to do that, you'll need to be part of the "Domain EXServers" security group.